A Report
to the
Montana
Legislature

Information Systems Audit

State Web Server Security Audit

Department of Administration

January 2008

Legislative Audit
Division

08DP-02

Legislative Audit Committee

Representatives

Bill Beck
Bill Glaser
Betsy Hands
Hal Jacobson, Vice Chair
John Sinrud
Bill Wilson

Senators

Joe Balyeat, Chair
Greg Barkus
Steve Gallus
Dave Lewis
Lynda Moss
Mitch Tropila

Audit Staff

Information Systems

Stephen Daem
Dale Stout

Fraud Hotline
Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at:

(Statewide)
1-800-222-4446
(in Helena)
444-4446

Information System Audits

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705
(406) 444-3122
Reports can be found in electronic format at:
http://leg.mt.gov/audit.htm

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
Tori Hunthausen,
Chief Deputy Legislative Auditor

Deputy Legislative Auditors:
James Gillett
Angie Grove

January 2008

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of the state's web server security. Web servers are used by the public to access state programs and services. The focus of the audit was to determine whether the state has controls in place to mitigate unauthorized activity on its web servers.

This report contains two recommendations for the development and implementation of controls, policies and standards to define and increase security on state web servers.

Respectfully submitted,

/s/ Scott A. Seacat

Scott A. Seacat
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

TABLE OF CONTENTS

Appointed and Administrative Officials

Department of Administration	Janet R. Kelly, Director
	Dick Clark, Chief Information Officer, Information Technology Services Division

Executive Summary

Background

A web server is a computer running software to provide services to other computers and their users. There are two types of web servers: external and internal. The state's external web servers are vital in allowing the public access to state programs and services. For example, many state citizens register for hunting licenses and permits through the Automated Licensing System. The state's internal web servers perform a wide array of functions including allowing user access to non-public agency applications and data. Both internal and external web server application security weaknesses potentially allow a user to gain unauthorized access to alter web site programming or agency data. Additionally, web servers could potentially be put into production without state authorization. Without proper controls, unauthorized access and servers could allow access to any data for any services offered through state web servers.

Audit Objectives, Scope, and Methodology

Our audit focused on the security of the state's web servers and its applications. Due to state services being vital to both state internal users and the public, our audit objective was to determine the state has controls in place to mitigate unauthorized web server activity. Our scope included both state external and internal servers with access to the state network. We interviewed Department of Administration (DOA) staff responsible for state network enterprise policy-making and agency network administrators to determine agency control environments regarding web servers and applications. We also reviewed contracts and statements of work to determine areas of responsibility for web servers. We scanned address ranges and compared the results to known web server addresses to determine the potential for unauthorized web servers. Security over web servers and applications was tested through scanning web servers and state agency web sites with automated software tools.

Conclusion

Based on our work, we determined enterprise-wide policy is vague and does not fully define agency web server and application security. This has led to agencies applying differing, or, in some cases, no web server or application security. For example, agencies are not scanning their web applications for security weaknesses to update the applications as required by DOA enterprise policy. We also determined DOA is not performing standard security checks on external web servers before the servers are made available to the public as required by the Department's enterprise security policies. Although our scans for unauthorized external web servers did not identify any unauthorized servers, we determined the risk posed by these servers is substantial and DOA does not perform

regular monitoring for these servers. DOA can strengthen controls over web server and application security by defining state web server and web server application security responsibilities in policy, notify agencies of these responsibilities, implement procedures to comply with enterprise web server and application policy and regularly monitor for unauthorized state external web servers.

Chapter I – Introduction and Background

Introduction to Web Servers

Every computer containing an Internet website must have a web server program. A web server is a computer running software to provide services to other computers and their users. This server may connect to agency databases and other system applications. There are two types of web servers: external and internal. External web servers are generally accessible to the public while internal servers are inside a network (inside the organization's external firewalls) and are only accessible to authorized individuals. The state network has both external and internal web servers.

External Web Servers

The state's external web servers are vital in allowing the public access to state programs and services. For example, many state citizens register for hunting licenses and permits through the Automated Licensing System.

Web server and application security weaknesses potentially allow a user to gain unauthorized access to resources or website programming. Unauthorized access allows the ability to alter website programming or alter agency data. Without proper controls, unauthorized access would allow access to any data for any services offered through the external web servers.

Internal Web Servers

The state's internal web servers perform a wide array of functions including allowing agency user access to the Statewide Accounting, Budgeting and Human Resources System (SABHRS), Montana Information Network for Employees (MINE) and non-public agency applications and data. State internal web servers are relied on by users to gain access necessary to perform their work. Internal web servers are subject to the same vulnerabilities as external web servers. However, an additional security weakness could exist. An individual with internal network access (such as a state, county or contractor employee) could set up a web server to communicate outside the state network without gaining authorization from the state; this is called a rogue server. Rogue servers bypass all state defenses, not only allowing the unauthorized passing of sensitive data outside the state network, but potentially leaving these servers open to the same vulnerabilities as external web servers.

Audit Objectives

The objective of our work focused on the security of the state's web servers and its applications. These systems are vital to the state by providing public accessibility to

state services. For example, many state citizens register for hunting licenses and permits through the Automated Licensing System. The importance of these services led to our audit objective to determine the state has controls in place to mitigate unauthorized web server activity.

Audit Scope and Methodology

The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office. We evaluated the control environment using state law, state enterprise security policies and Control Objectives for Information and related Technologies (COBIT).

The general public as well as state employees rely on both internal and external servers to provide access to Montana services and data. Through interview with Information Technology Services Division (ITSD) of the Department of Administration (DOA) network management and staff, we were able to determine the importance of both external and internal web servers in supplying those services and data. Also, prior to our audit, one agency's web site was compromised due to a test form that was left on a production web server. Once notified by the Department of Administration, the form was removed and the site secured. Therefore, our audit scope included statewide internal and external web servers with access to the state network. We interviewed DOA network staff responsible for state network enterprise policy-making and agency network administrators to determine agency control environments regarding web servers and applications. We reviewed contracts, statements of work, and evaluated the potential of rogue servers through scanning server address ranges and comparing the results to known servers. We also tested security over web servers and web applications through scanning web servers and agency web sites with automated software tools.

Conclusion

State agency web servers exist in varied environments throughout different agencies leading to different levels of web server and web application security management. Enterprise-wide policy for agency web server security exists, but responsibility is vague resulting in agencies interpreting web server security differently. Our audit determined web server and web application control weaknesses exist, potentially allowing loss of data and denial of access to web-based government services. The following sections report the results of our work.

Chapter II – Web Server and Applications Controls

Are State Web Servers Secure?

Web server security relies on the security of the server's software. Department of Administration (DOA) is charged by statute to create enterprise policy for the state's computer network. Enterprise Security policy ENT-SEC-012, Internet/Intranet Security, requires a web server to have a standard security check by an ITSD bureau before the server becomes available to the public. We determined ITSD is not performing this required initial check.

A common method of ensuring server software is secure is to run security weakness scanning software against the server to provide a list of weaknesses existing on that server. Although ITSD does not comply with ENT-SEC-012 in providing the required initial web server security check, they perform a monthly scan to determine if web server software security weaknesses exist. We scanned the same range of web server addresses as ITSD's monthly scan and determined, due to scanning software limitations, not all state web servers are being scanned by ITSD. We informed ITSD of the servers not included in their scans.

Enterprise Security policy ENT-SEC-022, Network Server Security, requires agencies ensure all server software is updated with the latest security patches and updates in a timely fashion. ITSD management asserted they do not believe all agencies are aware of agency responsibility to update or patch agency web servers and web applications. This lack of awareness was substantiated when we talked with ten agency network administrators regarding web site security. Two administrators stated they were informed by ITSD management not to perform any scanning.

Could State Data Walk Through The Door?

An unsecure web server application could allow unauthorized access to agency data. We scanned nine state web servers and four state web site addresses for web application security weaknesses and detected ten servers and web site addresses with weaknesses. All ten contained a total of 143 application weaknesses that, if exploited, could lead to:

- Identity theft.
- Loss of confidential data.
- Loss of public faith for the exploited agency.
- Lawsuits.
- Denial of public accessibility to government services.
- Spread of viruses and Trojan horses to individuals using government services.

Also during our testing we identified, on a public web site, details of three state web sites with application weaknesses. Details included the state web site addresses and the weaknesses. ITSD contacted the responsible agencies; as of December 19, 2007, the public web site still lists two of the state websites as not fixed.

Web server application security weaknesses may be prevented by scanning the applications. ENT-SEC-012 requires a web server go through a standard security check. However, this is not occurring, leaving the servers vulnerable to exploitation. Over time, web server applications become vulnerable to new, previously unknown, security deficiencies. This may be prevented by agencies keeping the web server application updated and patched to prevent exploitation as required by enterprise policy ENT-SEC-022. We interviewed network administrators from the ten agencies our scanning determined had web application weaknesses. None of the ten agencies we interviewed are fulfilling the requirements of ENT-SEC-022. The administrators indicated they are not performing web server application scans for the following reasons:

- Agencies were told by ITSD management not to do any scanning on the state network.
- Security testing has been left up to third party developers.
- Some agencies believe ITSD is responsible for web application security especially if the application is ITSD hosted.
- They believe their code reviews are sufficient.

Who Is Responsible For State Web Server Security?

Current policy over Internet/Intranet security (ENT-SEC-012) states standard security checks will be provided by an ITSD bureau before a server is made publicly available. However, the bureau was restructured in March 2007 and the policy has not been changed. The policy also does not define other web server security responsibilities such as:

- What the standard security check involves.
- What happens if a web server fails the check.
- Who is responsible for web server security.
- What web server security involves once the server becomes publicly available.

The state's web servers exist in varied environments throughout state agencies leading to different levels of web server security management. To provide an enterprise-wide expected level of security, ENT-SEC-012 is to guide agency web server responsibility. However, we determined state agencies do not know who is responsible for what part of web server and web server application security. We asked network administrators of the ten agencies our scanning determined had web application security weaknesses about the clarity of enterprise-wide policy regarding web server and web server application

security responsibilities. Seven responded policies were either vague or minimal, one had no comment, one said they followed best practices and one did not know a web server security policy existed.

The lack of defining web server and server application security responsibility has led to agencies applying differing or, in some cases, no web server or server application security. For example, among the ten agency network administrators we interviewed none scan their web applications for weaknesses, and four rely on reviewing application code. Three agencies also believe the security of any applications developed by third parties are the responsibility of the developer and three believe ITSD is responsible if the application is hosted on ITSD servers.

RECOMMENDATION #1

We recommend the Department of Administration:

A. Define state web server and web server application security responsibilities in policy.

B. Notify all state agencies of their web server and web server applications security responsibilities.

C. Implement procedures to comply with Enterprise Security policy ENT-SEC-012.

What Is This Server Doing Here?

Any web server created without authorization from the state is called a rogue server. Rogue servers can bypass all state defenses not only allowing the unauthorized passing of sensitive data outside the state network, but potentially leaving these servers open to the same security weaknesses as any other external or internal web server. This is of greater risk in a De-Militarized Zone (DMZ-the area between an external and internal firewall) where the rogue server would be able to communicate outside the state network. Our audit identified a potential for rogue web servers to be operating within the state's DMZ. The state does have controls in place to prevent rogue servers in the DMZ from connecting outside the state network. However, there are methods such as replacing an authorized web server with a rogue server that will allow the controls to be bypassed.

Common business practice is to implement procedures to monitor the network for unauthorized changes, including rogue servers. This monitoring can be accomplished by scanning the DMZ for any server not authorized for the DMZ. Currently, the state does not perform this scanning. During the audit we scanned the DMZ for rogue servers and did not detect any. However, the risk of a rogue server being placed in the DMZ

and communicating outside the state network as well as the server having the same vulnerabilities as any other web server is still substantial.

RECOMMENDATION #2

We recommend the Department of Administration scan the De-Militarized Zone for rogue servers on a regular basis.

Department of Administration

Department Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

BRIAN SCHWEITZER, GOVERNOR — JANET R. KELLY, DIRECTOR

STATE OF MONTANA

(406) 444-2032
FAX (406) 444-6194

MITCHELL BUILDING
125 N. ROBERTS, RM 155
PO BOX 200101
HELENA, MONTANA 59620-0101

January 11, 2008

RECEIVED
JAN 10 2008
LEGISLATIVE AUDIT DIV.

Mr. Scott Seacat, Legislative Auditor
Legislative Audit Division
State Capitol Building, Room 160
PO Box 201705
Helena, MT 59620-1705

RE: Information Systems Audit #08DP-02: State Web Server Security Audit

Dear Mr. Seacat:

The Department of Administration has reviewed the Information Systems Audit of the State Web Server Security and the recommendations contained therein. Our responses to the recommendations appear below:

Recommendation #1

We recommend the Department:

A. Define state web server and web server application security responsibilities in policy.
B. Notify all state agencies of their web server and web server applications security responsibilities.
C. Implement procedures to comply with Enterprise Security policy ENT-SEC-012

Response:

We concur.

A. The Department is currently drafting an Enterprise Information Systems Security Policy based on the requirements of MCA 2-15-114 "Security responsibilities of departments for their data."
B. The Department is implementing an Information Systems Security Program. This program will provide training for all agencies on risks, threats, and vulnerabilities enabling them to make proactive decisions about the security of their information assets and supporting systems.
C. Additional resources will be required to implement this recommendation. An EPP item will be submitted to the next legislative session.

Recommendation #2

We recommend the Department of Administration scan the De-Militarized Zone for rogue servers on a regular basis.

Response:

We concur. Additional guidance for this will come from the Enterprise Information Systems Security Policy and other related documents. Configuration management, with processes to ensure compliance, is needed at all levels within the Enterprise to ensure that no rogue devices exist. Any rogue device within or outside of the DMZ can have extreme consequences to the security of the state's information assets.

The Information Technology Services Division is defining and implementing a Network Operations Security Center (NOSC). The NOSC will provide rapid proactive diagnosis of security, server and network issues, analysis, and optimization.

Additional resources will be required to implement this recommendation. An EPP item will be submitted to the next legislative session.

My staff and I appreciate the courtesy and professionalism of the legislative audit staff in conducting this audit.

The Department's Corrective Action Plan (CAP) is enclosed.

Sincerely,

Janet R. Kelly, Director

Enclosure

Corrective Action Plan (CAP): Audit Report #08DP-02
State Web Server Security Audit
Department of Administration (DOA)
January 11, 2008

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**Recommendation #1** We recommend the Department: **A.** Define state web server and web server application security responsibilities in policy. **B.** Notify all state agencies of their web server and web server applications security responsibilities. **C.** Implement procedures to comply with Enterprise Security policy ENT-SEC-012	No		Concur	**A.** DOA is currently drafting an Enterprise Information Systems Security Policy based on the requirements of MCA 2-15-114 "Security responsibilities of departments for their data." **B.** The Department is implementing an Information Systems Security Program. This program will provide training for all agencies on risks, threats, and vulnerabilities enabling them to make proactive decisions about the security of their information assets and supporting systems. **C.** Additional resources will be required to implement this recommendation. An EPP item will be submitted to the next legislative session.	Dick Clark Dick Clark Dick Clark	3/1/08 9/1/08 9/1/09
61010 DOA	**Recommendation #2** We recommend the Department of Administration scan the De-Militarized Zone for rogue servers on a regular basis.	No		Concur	Additional guidance for this will come from the Enterprise Information Systems Security Policy and other related documents. Configuration management, with processes to ensure compliance, is needed at all levels within the Enterprise to ensure that no rogue	Dick Clark	3/1/08

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
					devices exist. Any rogue device within or outside of the DMZ can have extreme consequences to the security of the state's information assets.		
					ITSD is defining and implementing a Network Operations Security Center (NOSC). The NOSC will provide rapid proactive diagnosis of security, server and network issues, analysis, and optimization.	Dick Clark	9/1/08 (first phase)
					Additional resources will be required to implement this recommendation. An EPP item will be submitted to the next legislative session.	Dick Clark	9/1/09